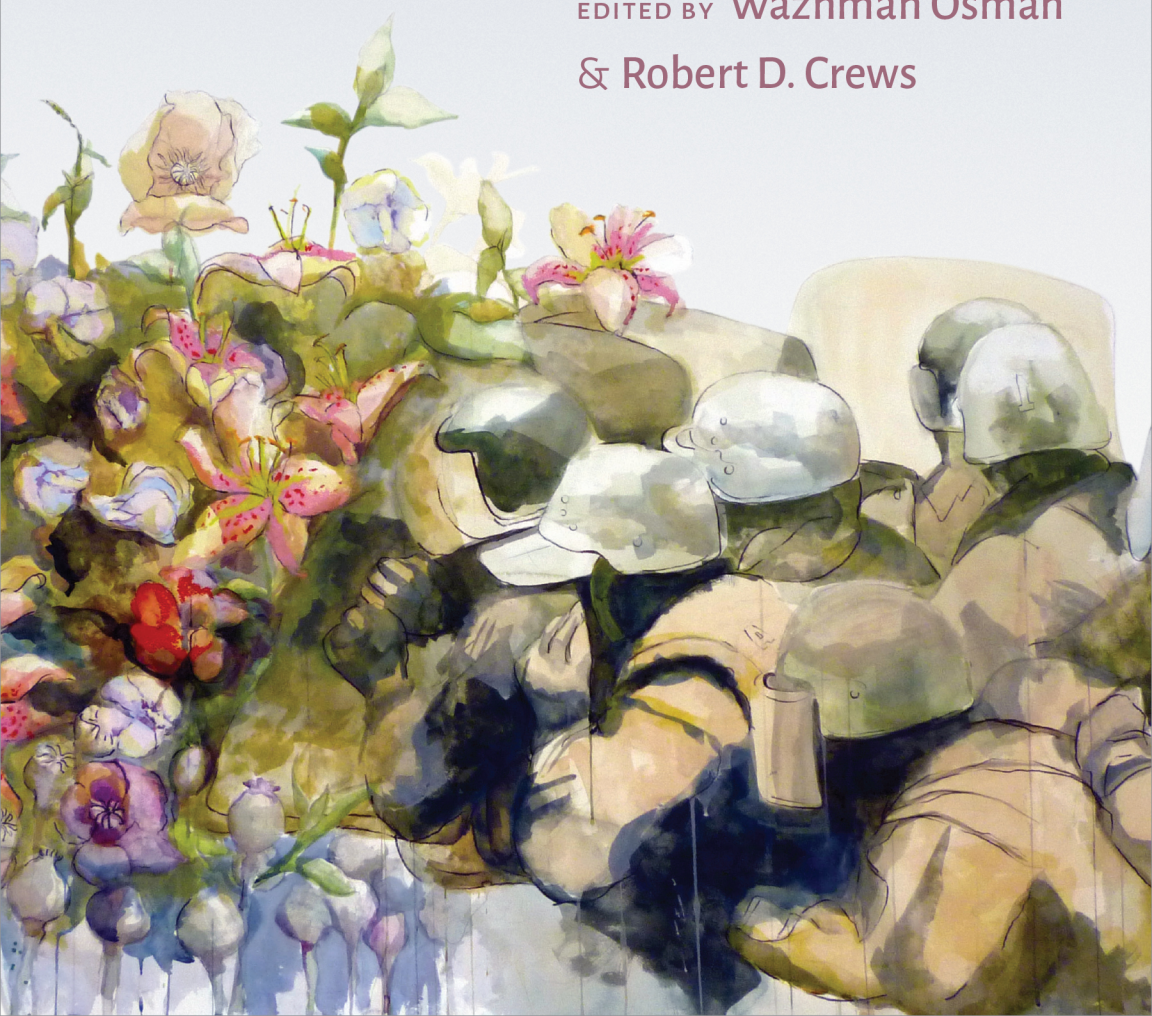


Decolonizing Afghanistan

Countering Imperial
Knowledge & Power

EDITED BY Wazmah Osman
& Robert D. Crews



Decolonizing Afghanistan

This page intentionally left blank

Decolonizing Afghanistan Countering Imperial Knowledge & Power

Edited by

WAZHMAH OSMAN AND ROBERT D. CREWS

DUKE UNIVERSITY PRESS *Durham and London* 2025

© 2025 DUKE UNIVERSITY PRESS

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, available at <https://creativecommons.org/licenses/by-nc-nd/4.0/>.

Printed in the United States of America on acid-free paper ∞

Project Editor: Ihsan Taylor

Designed by Matthew Tauch

Typeset in Arno Pro and General Sans

by Westchester Publishing Services

Library of Congress Cataloging-in-Publication Data

Names: Osman, Wazhmah, [date] editor. | Crews, Robert D., [date] editor.

Title: Decolonizing Afghanistan : countering Imperial knowledge and power / edited by Wazhmah Osman and Robert D. Crews.

Description: Durham : Duke University Press, 2025. | Includes bibliographical references and index.

Identifiers: LCCN 2025004854 (print)

LCCN 2025004855 (ebook)

ISBN 9781478032601 (paperback)

ISBN 9781478029229 (hardcover)

ISBN 9781478061427 (ebook)

ISBN 9781478094432 (ebook other)

Subjects: LCSH: Political stability—Afghanistan. | Violence—Afghanistan. | Afghanistan—Politics and government—21st century. | Afghanistan—History—2021- | Afghanistan—Social conditions—21st century. | Afghanistan—Population. | Afghanistan—Emigration and immigration—History—21st century.

Classification: LCC DS371.44 .D436 2025 (print) | LCC DS371.44 (ebook)

LC record available at <https://lcn.loc.gov/2025004854>

LC ebook record available at <https://lcn.loc.gov/2025004855>

Cover art: Laimah Osman, *They will be greeted by flowers . . .*, 2011 (detail). Graphite, colored pencils, and watercolor on Arches Watercolor Paper, 4 × 5 ft. Courtesy of the artist.

Tracking and Targeting

The US Surveillance Infrastructures in Afghanistan

Surveillance was a key part of the US war in Afghanistan. In two decades of occupation (2001–2021), the American military invested enormous resources into building a digital regime of tracking, targeting, and identification unprecedented in the history of war. These infrastructures of militarized knowledge included technologies of both geographical and population surveillance that offered American generals a synoptic view of the country from above and below. Yet despite the deployment of high-tech machines and sophisticated weapons, the American war in Afghanistan failed.

This failure exposed the limits of weaponized knowledge that serves the interest of colonial powers in subjugating the target population. As critical media scholars and scholars of colonial statecraft have shown, the history of surveillance and colonial domination are intertwined, and that relationship has been further strengthened in the digital age (Browne 2015; Hopkins 2020; Zureik 2020; M. Kaplan 1995; Nishiyama 2015; Gregory 2004; Weizman 2017). The US technological experiments in Afghanistan, therefore, can be best understood as part of a larger history of imperial construction of militarized knowledge in the Global South. In this chapter, I explore how the United States pursued its domination of Afghanistan through techniques and technologies of biometric identification.

In 2001, Americans knew little about Afghanistan. The country had been closed off for a quarter of a century (1978–2001) due to a series of political events that led to self-imposed isolation. The events included a Communist coup, the Soviet occupation, a civil war, and the Taliban

rule, which all happened in succession. In this period, Afghanistan was not exactly like North Korea, but it was close in terms of connections to the outside world beyond the Eastern Bloc. The country missed all the technological advancements that the world had achieved in this crucial quarter of a century. In 2000, for example, there were only two telephone lines in Afghanistan for international calls, both in the capital, Kabul—one at the Ministry of Communication and the other at the Central Post Office, where people from a handful of Western and neighboring countries could call or receive a call (*Shariat Weekly* 2000). The total number of telephone lines in the country was 35,200 in 2001 (the last year of the Taliban), a slight increase from 21,619 lines in 1978 (the year of the Communist rule). Most of these telephone lines were concentrated in Kabul. In 2001, for example, there was not a single telephone line in the provinces of Bamiyan, Farah, Nimroz, Helmand, Nuristan, and Badakhshan—not even in the government offices (*Annual Statistics Book* 2001, 202–220).

This was the state of information communication infrastructure in Afghanistan at the dawn of the new century. The Afghan state, or what was left of it after two decades of war, was a fragile institution with no functioning component parts. Most importantly, its memory was gone: There was not much of an archive where one could find information about the population. Most people had no identification documents or birth certificates, and the state had no way of knowing who was who (Karimi 2019, 4781–4783). This was the state of government institutions when Americans arrived with the mission to transform the country. They were now in charge of conquering this land, defeating insurgents, and building a functional state in which power would be transferred through free and fair elections. Despite all the costly efforts over the next two decades, the US mission failed. This chapter assesses America's knowledge infrastructure in Afghanistan by focusing on how biometric technology served as an instrument of domination. The purpose of this chapter is first to outline the extent of the American surveillance operations in Afghanistan and then to examine the epistemic contradiction inherent in mass surveillance programs: too much information and too little knowledge.

Machine-Readable Enemy: Biometric Data Collection

The US invasion of Afghanistan was the first major war of the twenty-first century. The use of advanced technologies of surveillance, reconnaissance, and targeting was a key part of Washington's strategy for winning the war. Surveillance, in particular, received a great deal of attention from the American military. Mick Ryan, an Australian general, after the fall of the Afghan government, told the *Economist* (2022): "You could put forward a thesis that Afghanistan was the most densely surveilled battlespace in the history of humankind." He was not wrong. The US military and its NATO partners viewed everyone in Afghanistan as potential targets, and they treated them as such. Drones, blimps, and satellites were watching and listening to them from the air, and biometric systems made them accessible on land. The aerial technologies of surveillance and strike, in particular, gave the US military's knowledge of Afghanistan a vertical nature that according to Lisa Parks (2015), Caren Kaplan (2018), Eyal Weizman (2017), and Derek Gregory (2018), has been the default mode of perception for imperial warfighting and population domination. The purpose of these forms of datafication was to create machine-readable targets and automate the work of identifying enemies.

In 2001, right after the US invasion of Afghanistan, one of the first problems the military faced was managing the large number of suspects that they rounded up. At the time, the US military had no automated record-keeping system to manage the detainees' information. Earlier that year, the Army's Battle Command Battle Laboratory had produced a biometric enrollment device called the Biometric Automated Toolset (BAT). It was already used once in Kosovo to build a database of local laborers that the US peacekeeping mission had hired at their bases (BIMA 2010, 5), but it had not yet been used in a combat setting. In 2002, the army shipped a BAT prototype to Afghanistan, which was used to collect and process the identity of the men detained in the country (Voelz 2016, 185–186). This was the first use case of the new tech during the war.

The use of a cutting-edge technology of identification in Afghanistan was a particularly significant development. The US military wanted to build a database of their own from scratch wherein every bit of data entered was produced by, and met the needs of, the Americans. This is, as other scholars have shown, a feature of imperial domination where the colonial power prefers its own (technological) ways of knowing over the indigenous

knowledge practices. This epistemic prejudice often harms the subjugated population by creating what Achille Mbembe calls “necropolitics”: a condition of ever-present violence imposed by a colonial power over a colonized people (Mbembe 2003, 12; see also Weizman 2017, 1–16; Osman 2020, 71–72; 2019, 159). Those Afghans who had hopes of using America’s advanced digital technology—such as biometric identification—as tools to strengthen state institutions soon realized that the United States was pursuing goals that were not necessarily aligned with the interests of the Afghan people. The Americans had no intention of using their technology outside the military realm. The program’s militaristic nature was exposed when people noticed that the Americans only collected the data of Afghan men assumed to be of fighting age—between fifteen and sixty-four (Shanker 2011). Such a program was not intended to build the capacity of the Afghan government to deliver public services.

The biometric program started as an instrument to manage the data of detainees and prisoners, but it quickly expanded. The US military would capture the biometric data of all who joined the Afghan army and police or applied to work as translators or laborers on military bases where foreign forces were housed. By 2012, more than 2.5 million people were recorded in biometric databases in Afghanistan (*Economist* 2012). Additionally, the US military captured the biometric data of almost any random person they encountered during a patrol, especially in rural areas. Indeed, it became an important part of the job of army personnel. American soldiers patrolling outside their bases were tasked with stopping every young man they came across and collecting their biometric data, which included a digital scan of their fingerprints, iris, and face (see figure 6.1). Collecting biometric enrollment data took at least half an hour for each person. One soldier handled the devices and several others stood guard until the complicated data entry was completed. An American soldier once complained: “I thought we were in Afghanistan to jump out of airplanes and kill Taliban. [But in practice,] we were on a beat, like local cops” (Jacobsen 2021, 9).

Identifying the enemy has always been a challenge for occupying forces in Afghanistan throughout its modern history. In the nineteenth century, when the British Empire conquered Kabul, they struggled with the same problem of figuring out who was the enemy. In the Second Anglo-Afghan War (1879–1880), the British paid spies to catch insurgents. They paid members of the public, too, between 50 and 120 rupees if they reported an insurgent. The economic incentive turned people against each other. Many ended up on the gallows and the lucky ones were locked up in a



6.1 US marine Nickolai Bautista, rifleman, Bravo Company, 1st Battalion, 7th Marine Regiment, uses a Biometric Enrollment and Screening Device to capture an Afghan man's iris scan during a mission in Helmand Province, Afghanistan, May 1, 2014. Photo: Sgt. Joseph Scanlan (Wikimedia Commons).

city caravanserai that the British had converted into a prison (Karimi 2020, 625–629). A century later, the Soviet army, who similarly faced public resistance as they occupied Afghanistan (1979–1989), had to come up with a method to distinguish friend from foe. Their puppet regime in Kabul was too weak to carry out this task and, instead, indiscriminately arrested, imprisoned, and killed people en masse to solve their problem, which, unsurprisingly, further escalated the fight against the Communists.

On October 8, 1978, people in Kabul woke up to the walls of the Ministry of Interior plastered with pages of paper. The papers contained the names of some five thousand people the regime had killed. The names were put up by President Hafiz Allah Amin, who came to power as the second Communist president after killing the first one, his predecessor Nur Muhammad Taraki, during a swift coup. Amin claimed that Taraki had killed all the victims whose names were posted on the wall. Many people had loved ones disappeared. A large crowd quickly gathered around the Ministry to look for the names of family members who had gone missing. Every few minutes, an anguished wail would rise from the crowd as someone found the name they had been dreading to find. After a couple of days, Amin took down the lists as it did not earn him popularity as he

had hoped (‘Azimi 1999, 123–125). The bare walls of the Ministry then only showcased the usual “revolutionary” slogans that at the time were calligraphed everywhere in Kabul. One said: “Those who plot in the dark, will be perished in the dark” (Sadat 2014).

The US military, however, had a technological approach to gathering intel about those who fought against it—this was, after all, a war in the age of the internet. They invested early on in building a digital infrastructure of identification and surveillance to not only know the enemy but keep track of them through telecom and aerial surveillance. Biometric technology, however, was the primary instrument that was used to identify what the enemy looked like—their faces, irises, and fingerprints. The type of detailed information that would make the British and the Soviets jealous. Despite the difference in approach, the task of identifying the population and classifying people into friends and foes remained a key area of concern for colonial governmentality in Afghanistan under all the three occupying armies. The Americans, in other words, were doing exactly what previous occupiers did, but with sleeker—and not necessarily less violent—tools.

Once the US military collected the biometric data, a team used it to create “digital dossiers” for each individual and put certain persons of interest on a watch list. The list was then loaded into handheld biometrics devices such as a BAT or Handheld Interagency Identity Detection Equipment (HIIDE) that could “provide immediate feedback if a unit encounters a potential threat on the battlefield or at a base entry point” (Buhrow 2010, 48). The US forces believed the program was a technology for “protecting the Afghan populace and ensuring that only insurgents are targeted.” (Buhrow 2010, 45). The whole program was part of a larger effort to create what the US government called a “social radar” for the purpose of total surveillance (González 2015, 8). Some of America’s NATO allies in Afghanistan had national restrictions when it came to collecting private information, but the United States itself imposed few limitations (Buhrow 2010). While biometrics could potentially deny anonymity to insurgents, it was not very helpful in preventing terror attacks (especially on Afghan people) or strengthening the capacity of the Afghan state.¹

The work was aligned with the American strategy of achieving “identity dominance,” defined as the ability “to know whether a person encountered by a warfighter is a friend or a foe” (Woodward 2005, 30). This required the knowledge of a person’s biometric data as well as names, aliases, past activities, and communication networks. According to a military handbook, “Every person who lives within an operational area should be identified

and fully biometrically enrolled with facial photos, iris scans, and all 10 fingerprints (if present)” (CALL 2011, 31). The war was reduced to surveillance, identification, and tracking. This focus on the datafication of the war was partly the result of media backlash against the military’s many mistakes, such as bombing the wrong house or arresting the wrong men (Savage et al. 2022; Sturcke 2008). The military decided that they could fix the problem with better technology. In 2017, US military officials bragged to the *New York Times* about the amount of data they considered before authorizing a strike, including the use of 3D models of targeted houses (Khan and Gopal 2017). This technosolutionist approach to profound ethical and political issues inherent in the occupation was a persistent feature of the US war in Afghanistan. The personal data that the United States collected was used, among other ends, to build secret security watch lists that held enormous power over the lives of ordinary Afghans because of how much US law enforcement agencies trusted these methods. It became common for Afghans to be wrongly denied visas or jobs after their names were flagged on one of the security watch lists (*Economist* 2012).

The Failure of the Biometric State

The US military outsourced part of the task of collecting biometric data to the Afghan government. It provided Afghan military institutions with the necessary technology, which significantly increased the amount of biometric data amassed in Afghanistan. Several military and civilian government institutions started to collect biometric data. The Afghan army and police, in particular, would take any opportunity to capture people’s biometric data. They did not leave even the dead alone: On June 21, 2012, Taliban gunmen raided Spugmai, a lakefront restaurant outside Kabul, killing more than twenty of the guests. After a long firefight, the Afghan forces finally gunned them down (Neuman 2012). When the soldiers entered the restaurant, ignoring all the blood and debris, they started to scan the eyes of the dead Taliban militants. They were in a rush because the biometric devices could reliably read the iris scan only up to six hours after death. They managed to identify one of the assailants, whose biometric data had been captured in Logar Province two years prior (*Economist* 2012). The biometric data that the Afghan government collected, most of it in military contexts, was then passed on to several US government agencies including



6.2 It was not only suspects but almost everyone in Afghanistan who could be subject to biometric registration. Here, Staff Sgt. John Silvia (*left*) and Senior Airman Bradley Rae (*right*), both from the 455th Expeditionary Security Forces Group Bravo Sector, US Air Force, are collecting biometric information from local Afghan women receiving medical services at Bagram Airfield, Afghanistan, December 2, 2012. Photo: Senior Airman Chris Willis (Wikimedia Commons).

the Department of Defense, Department of Homeland Security, and the FBI (*Economist* 2012).

In a country at war, with weak civil society institutions and vulnerable people struggling with violence and poverty, digital privacy and data sovereignty were not top priorities for most Afghans. Even the political sovereignty of the Afghan state, largely funded by the United States, was compromised by the American military's frequent disregard for local laws, making data sovereignty for ordinary citizens even less attainable. As Wazhmah Osman has noted, the Afghan government was in a "colony position" and in no way poised to stand up to its benefactors (2020, 67). This was a perfect environment to collect massive amounts of personal data with few legal constraints. The Edward Snowden files, for example, revealed that the National Security Agency recorded almost every phone call in Afghanistan (Nicks 2014). They did so because they could: They saw no barriers. In 2011, Afghanistan became "the only country in the world" to fingerprint and photograph everyone, both on arrival and departure,

who passed through their major airport (Nordland 2011). The biometric devices at Kabul International Airport were installed by US financing, and all the data they collected was fed into computers at the US Embassy in Kabul and from there shared with other US government agencies (Nordland 2011). This fetishistic data collection was further accelerated with each Afghan election, which required voters to enroll in a biometric program in order to prevent electoral fraud. Despite the data collection, the program failed to produce transparency in elections.²

One justification for the widespread use of biometrics in Afghanistan was the existence of corruption and fraud inside the government. Fraud, especially in the military, was indeed a significant problem and key reason behind the state's fragility. In 2016, according to one estimation, 40 percent of the Afghan security forces supposedly stationed in Helmand Province did not exist (SIGAR 2020, 4). This widespread problem became known as the "ghost" problem: There were ghost soldiers, police officers, teachers, schools, and so forth. These all referred to evidence of systemic corruption created by top-level Afghan officials to defraud international donors. The donors themselves, particularly the Americans, were also contributors to Afghan corruption (Chayes 2021). The corruption was especially bad in the security sector where the US spent between \$4 billion and \$5 billion a year to sustain the Afghan military (SIGAR 2020, 3). Afghan officials would present fake names to donors and receive funds for the salaries, meals, uniforms, and supplies of those "ghost" soldiers. After the fall of the government, the last minister of finance, Khalid Payenda, revealed that the ghost problem was one of the key reasons the Afghan military collapsed as the actual number of Afghan military personnel was just a fraction of what was on paper: "Many of us found out that we never had 120,000 soldiers. We did not have police and army that amounted to over 300,000. That was all a lie; we never reached those levels. My conclusion right now, [is that] at best, [there were] maybe 40 to 50 thousand. The rest were all ghosts" (Payenda 2021).

There was a contradiction at the heart of the Afghan information order: While the United States oversurveilled the country and collected all sorts of information about the place and its people, this did not necessarily mean that the Americans had more knowledge of the place and its people. This dilemma is common in surveillance states. When the state puts the entire population under mass surveillance it ends up amassing so much information that it cannot humanly handle or make sense of it. They end up wasting energy on aimlessly collecting data and archiving it. This

problem was revealed by Project Maven. In 2018, the Pentagon awarded Google a contract to build an AI program to sift through all the drone footage it had collected from war zones and identify targets. The contract was canceled after Google employees protested that they were not going to build an AI weapon (Shane and Wakabayashi 2018). In contrast, the type of information that leads to useful knowledge is often the information that states collect with the consent of the population. This includes tax data, census data, house numbering, health data, personal information on passports, and similar surveillance techniques and technologies that are participatory: People knowingly and willingly share personal data with the state. The data collected in a predatory way, like the US mass surveillance in Afghanistan, satisfies neither the state's insatiable thirst for information nor its need for practical knowledge—the kind essential for delivering public services.

In order to fight the corruption in the Afghan government payrolls, Washington turned to digital technology. They wanted to build a digital database of verifiable personal information about each individual who received a salary. At the same time, there was already another effort underway to build a digital personal database in Afghanistan for counterterrorism purposes. Therefore, there were two types of biometric databases that the Afghan government used: those that tracked salaried government personnel, both military and civilian, and those that tracked the members of the public for administrative purposes. The database for the military was called Afghan Personnel and Pay System and was funded by the US Department of Defense. It had data on 700,000 individuals dating back forty years (Bajak 2021). In 2018, an audit found that the system still had many problems with verifying the data, suggesting that payroll corruption—a major form of corruption in the military—was still an issue (Office of Inspector General 2019). This database was located at the Ministry of Defense and only authorized users had access to it. It is probable that the Taliban has since gained control of it.

The Ministry of Interior's biometric database, Afghan-Automated Biometric Identification System, also funded by the United States, was an umbrella project for all civilian biometric collection efforts. For everything from passports to public service jobs and university admission, applicants were required to enroll in the biometric database. Many top officials for years had siphoned off the security sector's budget and one can assume that they were not thrilled to see some technology get in the way of their lucrative schemes. The database was located at the Ministry's General

Directorate of Counter-Crimes, suggesting the American donors of the tech considered biometric, among other things, a crime-fighting technology (O'Brien 2010). In July 2020, two gunmen on a motorbike assassinated Mohammad Anwar Moniri, the director of the biometric center at the Ministry of Interior, outside his home in Kabul (*Ufuq News* 2020). We never learned who were behind the attack.

Selling digital technologies, such as biometric identification, to people in a fragile state with widespread instability and corruption is easy. The public, out of desperation, will embrace any solution that promises to end their problems. This was the situation in Afghanistan when the Americans arrived. The Afghans who supported the American biometric program in the country hoped that the advanced technology would help the Afghan state build capacity to deliver public services. There was, however, a naivety in the belief that Afghanistan's problems were only technological. This was a country under occupation where the state officials felt accountable only to their colonial patrons, not to the public. One cannot expect the rule of law and accountability to exist in such an environment, and, therefore, the idea of building a digital Afghan state run on biometric data was doomed from day one. In a country where foreign soldiers have full authority to take the lives of citizens, national sovereignty and state power have no meaning. Afghanistan's problem was too big to be solved by technology.

Conclusion

Mass surveillance creates only the illusion of knowledge. Despite all the surveillance from land and air, the massive amount of data the Americans collected in Afghanistan could not help them succeed in their mission—nor did it help build a functional Afghan state. The reason was simple: The United States collected the data for its own militarized objectives, not to serve the people of Afghanistan or strengthen Afghan state institutions. As seen in colonial projects across the Global South, imperial powers have historically exercised control through knowledge practices designed for domination. These colonial modes of knowing are fundamentally predatory, excluding subject populations from any meaningful participation in the production of knowledge. This exclusion, as decolonial scholars have noted, is the result of “a hierarchy of superior and inferior knowledge” that is inherent in colonial epistemology

(Grosfoguel 2007, 214). In the case of Afghanistan, the US military spent billions of dollars on high-tech, intrusive surveillance infrastructure but ignored investing in local institutions that could lead to an accountable state based on an impersonal bureaucracy and the rule of law, a state capable of delivering public services and settling disputes. The surveillance data collected by the US military not only failed to help the United States—and the Afghan state—it posed a serious threat to the safety of people in Afghanistan. In 2021, the Afghan government collapsed, and the Taliban took power, again. After two decades of bloodshed, the Americans replaced the Taliban with the Taliban. The new Taliban regime, technologically sophisticated and politically motivated, soon put to use all the surveillance infrastructures that they inherited from the Americans and the Afghan government.

The biometric infrastructures that the US built in Afghanistan harmed the public when the Americans were in the country and continue to harm them after they have left. The biometric databases stored at Afghan state institutions were always risky because of the weakness of the Afghan state and the threat of compromise. The US military, before their withdrawal, erased some of the biometric databases that the Afghan government maintained, especially the ones that stored the private information of the Afghan military personnel (Bajak 2021). The Taliban, however, have long been familiar with the importance of biometric data. They had managed to access the government's biometric devices even before the fall of the state. In some parts of the country, they would stop buses on the highway and subject passengers to biometric screening. In 2017, on one occasion, the Taliban identified ten members of the Afghan security forces on a bus and executed them on the spot (Kakar 2017; see also *Tolo News* 2016). The United States built a sophisticated surveillance infrastructure in Afghanistan that benefited no one, except for the Taliban. The group, according to local media, uses biometric technology to track down former employees of the Afghan government (Human Rights Watch 2022). Americans are gone from Afghanistan, but their legacy lives on.

Notes

- 1 On biometrics as a technology of identification, see Magnet (2011); Browne (2015); Gates (2011).
- 2 On this election, see the collection of detailed reports by Afghanistan Analyst Network, an independent think tank in Kabul (AAN 2020).

References

- AAN (Afghanistan Analysts Network). 2020. "AAN Dossier XXVII: Afghanistan's Contested 2019 Presidential Election and Its Aftermath." September 29. <https://www.afghanistan-analysts.org/en/dossiers/thematic-dossier-xxvii-afghanistans-contested-2019-presidential-election-and-its-aftermath/>.
- Annual Statistics Book 1380* [in Persian]. 2001. Kabul: Central Statistics Office.
- 'Azimi, Muhammad Nabi. 1999. *Urdu va Siyasat (Dar Sih Dahah-i Akhir-i Afghanistan)*. Peshawar: Mayvand.
- Bajak, Frank. 2021. "US-Built Databases a Potential Tool of Taliban Repression." *AP News*, September 7. <https://apnews.com/article/technology-business-taliban-coo7f85fb1b573c43a4391b947a5dcd4>.
- BIMA (Biometrics Identity Management Agency). 2010. "Introduction to Biometrics and Biometric Systems." US Army Corps of Engineers. <https://www.tam.usace.army.mil/portals/53/docs/udc/training/biometrics%20101.pdf>.
- Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.
- Buhrow, William C. 2010. "Using Biometrics in Afghanistan." *Army Magazine*, February. <https://www.ausa.org/sites/default/files/Buhrow.pdf>.
- CALL (Center for Army Lessons Learned). 2011. *Commander's Guide to Biometrics in Afghanistan: Observations, Insights, and Lessons*. CALL handbook. For official use only. Fort Leavenworth, KS: Center for Army Lessons Learned. <https://info.publicintelligence.net/CALL-AfghanBiometrics.pdf>.
- Chayes, Sarah. 2021. "Afghanistan's Corruption Was Made in America." *Foreign Affairs*, September 3. <https://www.foreignaffairs.com/united-states/afghanistans-corruption-was-made-in-america>.
- Economist*. 2012. "The Eyes Have It." July 7. <https://www.economist.com/asia/2012/07/07/the-eyes-have-it>.
- Economist*. 2022. "Where to Process Data, and How to Add Them Up." January 29. <https://www.economist.com/technology-quarterly/2022/01/29/where-to-process-data-and-how-to-add-them-up>.
- Gates, Kelly A. 2011. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: New York University Press.
- González, Roberto J. 2015. "Seeing into Hearts and Minds: Part 1. The Pentagon's Quest for a 'Social Radar.'" *Anthropology Today* 31 (3): 8–13.
- Gregory, Derek. 2004. *Colonial Present: Afghanistan, Palestine, Iraq*. Oxford: Blackwell.
- Gregory, Derek. 2018. "Eyes in the Sky—Bodies on the Ground." *Critical Studies on Security* 6 (3): 347–358.
- Grosfoguel, Ramón. 2007. "The Epistemic Decolonial Turn." *Cultural Studies* 21 (2–3): 211–223.

- Hopkins, Benjamin D. 2020. *Ruling the Savage Periphery: Frontier Governance and the Making of the Modern State*. Cambridge, MA: Harvard University Press.
- Human Rights Watch. 2022. "New Evidence That Biometric Data Systems Imperil Afghans." March 30. <https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans>.
- Jacobsen, Annie. 2021. *First Platoon: A Story of Modern War in the Age of Identity Dominance*. New York: Penguin.
- Kakar, Ajmal. 2017. "Taliban Subject Passengers to Biometric Screening." *Pajhwok News Agency*, February 14. <https://www.pajhwok.com/en/2017/02/14/taliban-subject-passengers-biometric-screening>.
- Kaplan, Caren. 2018. *Aerial Aftermaths: Wartime from Above*. Durham, NC: Duke University Press.
- Kaplan, Martha. 1995. "Panopticon in Poona: An Essay on Foucault and Colonialism." *Cultural Anthropology* 10 (1): 85–98.
- Karimi, Ali. 2019. "Surveillance in Weak States: The Problem of Population Information in Afghanistan." *International Journal of Communication* 13:4778–4794.
- Karimi, Ali. 2020. "The Bazaar, the State, and the Struggle for Public Opinion in Nineteenth-Century Afghanistan." *Journal of the Royal Asiatic Society* 30 (4): 613–633.
- Khan, Azmat, and Anand Gopal. 2017. "The Uncounted." *New York Times Magazine*, November 16. <https://www.nytimes.com/interactive/2017/11/16/magazine/uncounted-civilian-casualties-iraq-airstrikes.html>.
- Magnet, Shoshana Amielle. 2011. *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham, NC: Duke University Press.
- Mbembe, Achille. 2003. "Necropolitics." *Public Culture* 15 (1): 11–40.
- Neuman, Scott. 2012. "Taliban Attack Kills 21 At Lakeside Resort Near Kabul." *NPR*, June 22. <https://www.npr.org/sections/thetwo-way/2012/06/22/155560427/taliban-attack-kills-18-at-lakeside-resort-near-kabul>.
- Nicks, Denver. 2014. "WikiLeaks Claims Afghanistan Under NSA Surveillance." *Time*, May 23. <https://time.com/109853/wikileaks-afghanistan-under-nsa-surveillance/>.
- Nishiyama, Hidefumi. 2015. "Towards a Global Genealogy of Biopolitics: Race, Colonialism, and Biometrics Beyond Europe." *Environment and Planning D: Society and Space* 33 (2): 331–346. <https://doi.org/10.1068/d19912>.
- Nordland, Rod. 2011. "Afghanistan Has Big Plans for Biometric Data." *New York Times*, November 19. <https://www.nytimes.com/2011/11/20/world/asia/in-afghanistan-big-plans-to-gather-biometric-data.html>.
- O'Brien, William. 2010. "Conference Maps the Way Ahead for Biometrics in Afghanistan." Press release. US Central Command, October 15. <https://www.centcom.mil/MEDIA/PRESS-RELEASES/Press-Release-View/Article/903841/conference-maps-the-way-ahead-for-biometrics-in-afghanistan/>.

- Office of Inspector General. 2019. "Audit of the Planning for and Implementation of the Afghan Personnel and Pay System DODIG-2019-115." US Department of Defense, August 15. <https://www.dodig.mil/reports.html/Article/1937240/audit-of-the-planning-for-and-implementation-of-the-afghan-personnel-and-pay-sy/>.
- Osman, Wazhmah. 2019. "Racialized Agents and Villains of the Security State: How African Americans Are Interpellated against Muslims and Muslim Americans." *Asian Diasporic Visual Cultures and the Americas* 5 (1-2): 155-182.
- Osman, Wazhmah. 2020. *Television and the Afghan Culture Wars: Brought to You by Foreigners, Warlords, and Activists*. Urbana: University of Illinois Press.
- Parks, Lisa. 2015. "Vertical Mediation: Geospatial Imagery and the US Wars in Afghanistan and Iraq." In *Mediated Geographies and Geographies of Media*, edited by Susan P. Mains, Julie Cupples, and Chris Lukinbeal, 159-175. Dordrecht, Netherlands: Springer.
- Payenda, Khalid. 2021. "The Khalid Payenda Interview (1): An Insider's View of Politicking, Graft and the Fall of the Republic." Afghanistan Analysts Network, September 27. <https://www.afghanistan-analysts.org/en/reports/economy-development-environment/the-khalid-payenda-interview-1-an-insiders-view-of-politicking-graft-and-the-fall-of-the-republic/>.
- Sadat, Mir 'Abd al-Vahid. 2014. "Ihqaq-i Huquq-i Mardum va Ya Itlaf-i An." *Hod*, August 12. <http://howd.org/likene/211-2014-12-08-20-46-00.html>.
- Savage, Charlie, Eric Schmitt, Azmat Khan, Evan Hill, and Christoph Koettl. 2022. "Newly Declassified Video Shows U.S. Killing of 10 Civilians in Drone Strike." *New York Times*, January 19. <https://www.nytimes.com/2022/01/19/us/politics/afghanistan-drone-strike-video.html>.
- Shane, Scott, and Daisuke Wakabayashi. 2018. "'The Business of War': Google Employees Protest Work for the Pentagon." *New York Times*, April 4. <https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html>.
- Shanker, Thom. 2011. "U.S. Military Uses Biometrics to Identify People." *New York Times*, July 13. <https://www.nytimes.com/2011/07/14/world/asia/14identity.html>.
- Shariat Weekly*. 2000. "Announcement of the Afghan Wireless Company" [in Persian]. March 5.
- SIGAR (Special Inspector General for Afghanistan Reconstruction). 2020. *Quarterly Report to the United States Congress*. Accessed October 15, 2022. <https://www.sigar.mil/pdf/quarterlyreports/2020-07-30qr-intro-section1.pdf>.
- Sturcke, James. 2008. "US Air Strike Wiped out Afghan Wedding Party, Inquiry Finds." *Guardian*, July 11. <https://www.theguardian.com/world/2008/jul/11/afghanistan.usa>.

- Tolo News*. 2016. "Taliban Used Biometric System During Kunduz Kidnapping." June 5. <https://www.tolonews.com/afghanistan/taliban-used-biometric-system-during-kunduz-kidnapping>.
- Ufuq News*. 2020. "Mudir-i sistim-i bayumitrik-i vizarat-i dakhilah dar Kabul kushtah shud." July 8. <https://ufuqnews.com/archives/154005>.
- Voelz, Glenn. 2016. "Catalysts of Military Innovation: A Case Study of Defense Biometrics." *Defense Acquisition Research Journal* 23 (2): 178–201.
- Weizman, Eyal. 2017. *Hollow Land: Israel's Architecture of Occupation*. New ed. London: Verso.
- Woodward, John D., Jr. 2005. "Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism." *Military Review* 85 (5): 30–34.
- Zureik, Elia. 2020. "Settler Colonialism, Neoliberalism and Cyber Surveillance: The Case of Israel." *Middle East Critique* 29 (2): 219–235.